The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/13/2016

SUBJECT:
Multiple Vulnerabilities in Microsoft Office Could Allow For Remote Code Execution (MS16-107)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could result in remote code execution if the user opens a specifically crafted Microsoft Office file. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Microsoft Office 2007, 2010, 2013, 2013 RT, 2016
- Microsoft Office for Mac 2011, Office 2016 for Mac
- Microsoft Office Compatibility Pack SP3
- Microsoft Word Viewer
- Microsoft Excel Viewer
- Microsoft PowerPoint Viewer
- Microsoft SharePoint Server 2007, 2010, 2013
- Microsoft Office Web Apps 2010, 2013
- Microsoft Office Online Server

RISK:
Government:
- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could allow for remote code execution if a user opens a specially crafted Microsoft Office file.

- Ten memory corruption vulnerabilities exist when Microsoft Office fails to properly handle objects in memory. (CVE-2016-3357, CVE-2016-3358, CVE-2016-3359, CVE-2016-3360, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363, CVE-2016-3364, CVE-2016-3365, CVE-2016-3381)
- An information disclosure vulnerability exists when Visual Basic macros in Office improperly exports a user's private key from the certificate store while saving a document. (CVE-2016-0141)
- An information disclosure vulnerability exists in the way that the Click-to-Run (C2R) components handle objects in memory. (CVE-2016-0137)
- A spoofing vulnerability exists when Microsoft Outlook does not strictly adhere to RFC2046, and improperly identifies the end of a MIME attachment. An improper MIME attachment ending may cause antivirus or antispam scanning to not work as intended. (CVE-2016-3366)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://technet.microsoft.com/en-us/library/security/ms16-107.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0137
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0141
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3357
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3358
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3359
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3360
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3361

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3362
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3363
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3364
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3365
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3366
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3381

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/